HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/892,371	06/27/2001	Marcus Peinado	MSFT-0310/164266.1	2356

41505 7590 03/08/2005

WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE - 46TH FLOOR
PHILADELPHIA, PA 19103

EXAMINER	
HO, THOMAS M	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 03/08/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/892,371	**Applicant(s)** PEINADO, MARCUS	
	Examiner Thomas M Ho	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *27 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *23-35* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date #2 .

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-35 are pending.

Election/Restrictions

2. Restriction to one of the following inventions is required under 35 USC 121.

I. Claims 1-22 are drawn to a method of exchanging or distributing a license with a key embedded in class 380, subclass 278, key exchange.

II. Claims 23-35 are drawn to a method of authenticating using a nonce in class 713, subclass 170, authentication of an entity and a message.

Invention I has a separate utility as a license distributing system, where the license is structured to involve key distribution, such as in a system for content distribution.

Invention II has a separate utility as a method for authenticating a party with a nonce, otherwise known in the art as a randomly or pseudo-random value exchanged for authentication purposes. An example of this is a password or logon system to an email server.

These inventions are distinct for the reasons given above and while related to the field of computer security, embody independent inventions within that field and would consequently require different searches in their different subclasses.

Invention I would require a separate search of class 380, subclass 278.

Invention II would require a separate search of class 713, subclass 170.

A telephone call was conducted with Mr. Steven, Meyer, the applicant's representative, on March 4th, 2005 to address the possibility of a restriction election.

The applicant selected group I without traverse.

Claims 1-22 are now presented for examination.

Claims 23-35 are withdrawn from consideration.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1, 3-6, 8-9, 11, 13-14 is rejected under 35 U.S.C. 102(b) as being anticipated by Saito, US patent 6,002,772.

In reference to claim 1:

Saito discloses a method for rendering encrypted digital content on a first device having a public key (PU1) and a corresponding private key (PR1), the digital content being encrypted according to a content key (KD), the method comprising:

- Obtaining a digital license corresponding to the content, the digital license including the content key (KD) therein in an encrypted form, where the digital license is obtained by generating at the data management center the combination of content keys Ks1 with the content name, first user data, and first user public key. (Column 6, lines 60-67)
- Decrypting the encrypted content key (KD) from the digital license to produce the content key (KD), where the content keys are decrypted from the digital license. (Column 7, lines 5-10)
- Obtaining from the first device the public key thereof (PU1), where the first device is the first user, and the data management center obtains the public key where the user presents the key and requests distribution of secret keys. (Column 6, lines 43-47)
- Encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)), where the content key Ks1 is encrypted with the public key. (Column 6, lines 60-67)
- Composing a sub-license corresponding to and based on the obtained license, the sub license including (PU1 (KD)), and transferring the composed sublicense to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and can render the encrypted content on the first device with the produced content key(KD), where the sub-

license is the encrypted secret keys which are transferred to the first device, or first user. (Column 7, lines 2-5), and the sub-license may then be decrypted to produce the content key, Ks1.

In reference to claim 3:

Saito discloses the method of claim 1 further comprising transferring the content to the first device, where the data content is supplied to the first user. (Column 5, lines 14-20)

In reference to claim 4:

Saito discloses the method of claim 1 for rendering encrypted digital content on a first device having a digital rights management system(DRM), the DRM system having the public key(PU1), where the DRM is the system used in Saito (Column 6, lines 20-22) and the corresponding private key (PR1), the method comprising:

- Obtaining from the first device the public key of the DRM system thereof(PU1), where the user presents the key and requests distribution of secret keys. (Column 6, lines 43-47)
- Encrypting the content key (KD) according to the public key (PU1) of the DRM system of the first device (PU1 (KD)), where the content key Ks1 is encrypted with the public key. (Column 6, lines 60-67)
- Composing a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD)), and transferring of the composed sub-license to the first device, wherein the DRM system of the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD), and

can render the encrypted content on the first device with the produced content key (KD), where the sub-license is the encrypted secret keys which are transferred to the first device, or first user. (Column 7, lines 2-5), and the sub-license may then be decrypted to produce the content key, Ks1.

In reference to claim 5:

Saito discloses the method of claim 1 comprising:

- Obtaining the digital license and storing the obtained digital license on a second device, where the digital license is combination of the Cks2Kb2, and Cks3kb2, and where the second device is the second user (Column 9, lines 8-17)
- Decrypting the encrypted content key (KD) from the digital license on the second device to produce the content key (KD), where the content keys are decrypted (Column 9, lines 19-26)
- Obtaining from the first device the public key thereof (PU1), where the first user presents the public key and the data center obtains it from the first user in this manner. (Column 6, lines 43-47)
- Encrypting the content key (KD) according to the public key (PU1) of the first device (PU1 (KD)), where the content key Ks1 is encrypted with the public key. (Column 6, lines 60-67)
- Composing a sub-license corresponding to and based on the obtained license, the sub-license including (PU1 (KD)), and transferring the composed sub-license from the second device to the first device, wherein the first device can decrypt (PU1 (KD)) with the private key thereof (PR1) to produce the content key (KD),

and can render the encrypted content on the first device with the produced content key(KD), where the sub-license is the encrypted secret keys which are transferred to the first device, or first user. (Column 7, lines 2-5), and the sub-license may then be decrypted to produce the content key, Ks1.

In reference to claim 6:

Saito discloses the method of claim 5 wherein the second device has a public key (PU2) and a corresponding private key (PR2), the method comprising:

- Obtaining a digital license corresponding to the content, the digital license including the content key (KD) encrypted according to the public key (PU2) of the second device (PU2 (KD)), where the content key is encrypted with a second public key and where the digital license is combination of the Cks2Kb2, and Cks3kb2, and where the second device is the second user (Column 9, lines 8-17)
- Decrypting (PU2(KD)) from the digital license according to the private key (PR2) of the second device to produce the content key (KD), where the content keys are decrypted (Column 9, lines 19-26)

In reference to claim 8:

Saito (Column 7, lines 15-20) discloses the method of claim 1 wherein, the first device is a portable device, where the device is an IC card or PCMCIA card.

In reference to claim 9:

Saito discloses the method of claim 1 wherein obtaining from the first device the public key record thereof(PU1) comprises receiving a certificate from the first device within which is (PU1), where the user presents the key along with user data. (Column 6, lines 43-47), and it is understood in the art that a digital certificate typically comprises user identification data and the public key.

In reference to claim 11:

Saito discloses the method of claim 9 comprising receiving a certificate from the first device within which is (PU1) and information relating to the first device, where the user presents the key along with user data. (Column 6, lines 43-47), and it is understood in the art that a digital certificate typically comprises user identification data and the public key.

Claim 13 is rejected for the same reasons as claim 11.

In reference to claim 14:

Saito discloses the method of claim 11 further comprising obtaining (PU1 (KD)) from the transferred sub-license(Column 7, lines 2-5), applying (PR1) to (PU1 (KD)) to obtain the content key (KD) , and applying (KD) to decrypt the encrypted content, all by the first device. (Column 7, lines 5-13)

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 2, 7, 10, 12, 15-22 are rejected in view of Sato, US patent 6,002,772.

In reference to claim 2:

Saito fails to disclose the method of claim 1 further comprising, prior to composing the sub-license and transferring the composed sub-license to the device, checking the obtained license to determine that such license permits issuance of the sub-license to the device.

The Examiner takes official notice that authenticating users through user submitted personal information was well known in the art at the time of invention.

Saito however discloses that information regarding the user identity is submitted. While it is not explicitly stated that the data management center users this information to verify the identity of the user, it would have been obvious to one of ordinary skill in the art at the time of invention to authenticate the user with the user submitted data to make ensure the content wouldn't be submitted to someone without the proper credentials.

In reference to claim 7:

Saito fails to explicitly discloses the method of claim 5 wherein the second device is a computer.

The Examiner takes official notice that using computers for data content distribution was well known in the art at the time of invention.

It would have been obvious to one of ordinary skill in the art to distribute the data to a computer, provided the extra processing power a computer has over other electronic devices such as calculators.

In reference to claim 10:

Saito fails to discloses the method of claim 9 further comprising comparing the received certificate against a revocation list to ensure that the certificate has not been compromised.

The Examiner takes official notice that checking to see if a certificate has been compromised against a list was well known at the time of invention. This technology, known as CRLs or certificate revocation lists is a list that is passed around or stationary on a server, that computers may use to determine the "Freshness" of a given certificate. Examples of prior art that use CRLs are patents:

5717757, 5666416, 5793868.

It would have been obvious to one of ordinary skill in the art at the time of invention to check if a certificate was valid against a list in order to determine whether the information the user was providing was up to date.

Claim 12 is rejected for the same reasons as claim 2.

In reference to claim 15:

Saito discloses a method for rendering encrypted digital content on a first device having a public key (PU1) and a corresponding private key (PR1), the digital content being encrypted according to a content key (KD), the method comprising:

- Providing the public key (PU1) to a second device, wherein the second device obtains a digital license corresponding to the content, the digital license including the content key (KD), encrypts the content key (KD) according to the public key(PU1) of the first device (PU1, (KD)) and composes a sublicense corresponding to and based on the obtained license, the sub-license corresponding to and based on the obtained license, the sub-license including (PU1, (KD)), where the second device is the data center, and where the
- Receiving the composed sub-license from the second device, where the composed sub-license is created and sent tot he user. (Column 7, lines 3-5)
- Obtaining (PU1 (KD)) from the received sub-license (Column 7, lines 5-12)
- Applying (PR1) to (PU1 (KD)) to obtain the content key(KD) (Column 7, lines 5-12)
- Applying (KD) to decrypt the encrypted document, where Ks1 is used to decrypt the content. (Column 6, lines 43-46)

Saito fails to explicitly disclose rendering the decrypted document

The Examiner takes official notice that rendering digital content was well known at the time of invention.

It would have been obvious to one of ordinary skill in the art to render to the content of Saito in order to take advantage of the fact that that is what the content is there for.

In reference to claim 16:

Saito discloses the method of claim 15 further comprising receiving the content from the second device, where the second device is the data center, and the content is received by the first user. (Column 5, lines 15-20)

Claim 17 is rejected for the same reasons as claim 15.

Claim 18 is rejected for the same reasons as claim 7.

Claim 21 is rejected for the same reasons as claim 2, where the second device is the data center.

Claim 19 is rejected for the same reasons as claim 8.

Claim 20 is rejected for the same reasons as claim 11, where the second device is the data center.

Claim 22 is rejected for the same reasons as claim 11, where the second device is the data center.

Conclusion

7. Any inquiry concerning this communication from the examiner should be directed to Thomas M Ho whose telephone number is (571)272-3835. The examiner can normally be reached on M-F from 9:30 AM - 6:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (571)272-3838.

The Examiner may also be reached through email through Thomas.Ho6@uspto.gov

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist	Telephone: 571-272-2100	Fax: 703-872-9306
Customer Service Representative	Telephone: 571-272-2100	Fax: 703-872-9306

TMH

February 23rd, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER